

JASON M. WUCETICH (STATE BAR NO. 222113)
jason@wukolaw.com
DIMITRIOS V. KOROVILAS (STATE BAR NO.
247230)
dimitri@wukolaw.com
WUCETICH & KOROVILAS LLP
222 N. Pacific Coast Hwy., Suite 2000
El Segundo, CA 90245
Telephone: (310) 335-2001
Facsimile: (310) 364-5201

Attorneys for Plaintiff
JOSHUA STRADINGER, as an individual and on
behalf of all others similarly situated

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

JOSHUA STRADINGER, as an
individual and on behalf of all others
similarly situated,

Plaintiff,

v.

PROSPECT MEDICAL
HOLDINGS, INC.; and DOES 1-10,

Defendants.

CASE NO.

CLASS ACTION

COMPLAINT FOR:

- (1) NEGLIGENCE
- (2) NEGLIGENCE PER SE
- (3) DECLARATORY JUDGMENT
- (4) VIOLATION OF THE CAL.
CONFIDENTIALITY OF
MEDICAL INFORMATION ACT,
CAL. CIV. CODE § 56
- (5) VIOLATION OF THE CAL.
CUSTOMER RECORDS ACT,
CAL. CIV. CODE § 1798.84
- (6) VIOLATION OF THE CAL.
UNFAIR COMPETITION LAW,
CAL. BUS. & PROF. CODE §
17200
- (7) VIOLATION OF THE RIGHT TO
PRIVACY, CAL. CONST. ART. 1,
§ 1

DEMAND FOR JURY TRIAL

SUMMARY OF THE CASE

1
2 1. This putative class action arises from Prospect Medical Holdings,
3 Inc.'s (hereinafter "PMH") negligent failure to implement and maintain reasonable
4 cybersecurity procedures that resulted in a data breach of its systems on or around
5 July 31, 2023 through August 3, 2023. Plaintiff brings this class action complaint
6 to redress injuries related to the data breach, on behalf of himself and a nationwide
7 class and California subclass of similarly situated persons. Plaintiff asserts claims
8 on behalf of a nationwide class for negligence, negligence per se, declaratory
9 judgment, and common law invasion of privacy. Plaintiff also brings claims on
10 behalf of a California subclass for violation of the California Confidentiality of
11 Medical Information Act ("CMIA"), Cal. Civ. Code § 56, the California Customer
12 Records Act, Cal. Civ. Code § 1798.80 *et seq.*, violation of the California Unfair
13 Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*, and for invasion of
14 privacy based on the California Constitution, Art. 1, § 1. Plaintiff seeks, among
15 other things, compensatory damages, statutory damages, injunctive relief,
16 attorneys' fees, and costs of suit.

PARTIES

17
18 2. Plaintiff Joshua Stradinger is a citizen and resident of the State of
19 California whose personal identifying information was part of the July 31, 2023
20 through August 3, 2023 data breach that is the subject of this action.

21 3. On information and belief, defendant Prospect Medical Holdings, Inc.
22 is a corporation organized and existing under the laws of the State of Delaware,
23 with corporate headquarters located at 3415 S. Sepulveda Blvd., Los Angeles, CA
24 90034.

25 4. Plaintiff brings this action on behalf of himself, on behalf of the
26 general public as a Private Attorney General pursuant to California Code of Civil
27 Procedure § 1021.5 and on behalf of a class and subclass of similarly situated
28 persons pursuant Federal Rule of Civil Procedure 23.

JURISDICTION & VENUE

5. This Court has general personal jurisdiction over PMH because, at all relevant times, the company had systematic and continuous contacts with the State of California. PMH is registered to do business in California with the California Secretary of State. Defendant regularly contracts with a multitude of businesses, organizations and consumers in California to provide medical and health care related services. PMH does in fact actually provide such continuous and ongoing medical and health care related services to such customers in California and has employees in California.

6. Furthermore, this Court has specific personal jurisdiction over PMH because the claims in this action stem from its specific contacts with the State of California — namely, PMH’s provision of medical and health care related services to a multitude of customers in California, PMH’s collection, maintenance, and processing of the personal data of Californians in connection with such services, including but not limited to PMH’s employees, PMH’s failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent cybersecurity attack and security breach of such data in July and August 2023.

7. This Court has diversity subject matter jurisdiction under 28 U.S.C. § 1332(d) in that the matter in controversy exceeds the sum or value of \$5,000,000, exclusive of interests and costs, and is a class action in which members of the class defined herein include citizens of a State different from the PMH. Specifically, Defendant is a citizen of the state of California and the plaintiff class and/or subclasses defined herein include citizens of other states, including California.

8. Venue is proper in the Central District of California under 28 U.S.C. § 1391 (b)(1)-(2) and (c)(2) because a substantial part of the events or omissions giving rise to the claims alleged herein occurred within this judicial district, specifically PMH’s provision of medical and health care related services in

1 California and within Los Angeles County, PMH's collection, maintenance, and
2 processing of the personal data of Californians in connection with such services,
3 PMH's failure to implement and maintain reasonable security procedures and
4 practices with respect to that data, and the consequent security breach of such data
5 in July and August 2023 that resulted from PMH's failure. In addition, Plaintiff is
6 informed and believes and thereon alleges that members of the class and subclass
7 defined below reside in the Central District, and PMH has its corporate
8 headquarters within the Central District.

9 **FACTUAL BACKGROUND**

10 9. PMH is a group of more than 11,000 physicians and 18,000 employees
11 providing health care services at 16 different hospitals across 5 states. PMH
12 provides comprehensive health care services to its approximately 600,000
13 members.

14 10. In connection with these medical and health care related services,
15 PMH collects, stores, and processes sensitive personal data for thousands of
16 individuals, including but not limited to its employees, patients, members and
17 customers. In doing so, PMH retains sensitive information including, but not
18 limited to, bank account information, health care related information, addresses,
19 and social security numbers, among other things.

20 11. As a corporation doing business in California and having employees
21 and customers in California, PMH is legally required to protect personal
22 information from unauthorized access, disclosure, theft, exfiltration, modification,
23 use, or destruction.

24 12. PMH knew that it was a prime target for hackers given the significant
25 amount of sensitive personal information processed through its computer data and
26 storage systems. PMH's knowledge is underscored by the massive number of data
27 breaches that have occurred in recent years.

28 13. Despite knowing the prevalence of data breaches, PMH failed to

1 prioritize data security by adopting reasonable data security measures to prevent
2 and detect unauthorized access to its highly sensitive systems and databases. PMH
3 has the resources to prevent a breach, but neglected to adequately invest in data
4 security, despite the growing number of well-publicized breaches. PMH failed to
5 undertake adequate analyses and testing of its own systems, training of its own
6 personnel, and other data security measures as described herein to ensure
7 vulnerabilities were avoided or remedied and that Plaintiff's and class members'
8 data were protected.

9 14. Specifically, on or around August 1, 2023, PMH learned of a data
10 security incident that disrupted the operations of some of its IT servers. Upon
11 investigation, PMH learned that an unauthorized party gained access to its IT
12 network between the dates of July 31, 2023 and August 3, 2023. While in the
13 network, the unauthorized party accessed and/or acquired files that contained
14 personal identification information and/or personal health information of Plaintiff
15 and Class Members.

16 15. On information and belief, the personal information PMH collects and
17 which was impacted by the cybersecurity incident includes individuals' name,
18 social security number, date of birth, diagnosis information, lab results, prescription
19 information, treatment information, health insurance information, claims
20 information, and medical record number, among other personal, sensitive and
21 confidential information.

22 16. On or around September 29, 2023, PMH mailed data breach notices to
23 impacted parties. According to notice mailed to impacted individuals, the breach
24 resulted in individuals' name, social security number, date of birth, diagnosis
25 information, lab results, prescription information, treatment information, health
26 insurance information, claims information, and medical record number, among
27 other personal, sensitive and confidential information, was compromised and
28 acquired by unknown third parties. Plaintiff received a copy of a September 29,

1 2023 data breach notice via United States mail service confirming that his personal
2 identifying information was part of the data breach.

3 17. Upon information and belief, the parties responsible for the data
4 breach stole the personal information of all PMH's customers and employees,
5 including Plaintiff's. Because of the nature of the breach and of the personal
6 information stored or processed by PMH, Plaintiff is informed and believes that all
7 categories of personal information were further subject to unauthorized access,
8 disclosure, theft, exfiltration, modification, use, or destruction. Plaintiff is informed
9 and believes that criminals would have no purpose for hacking PMH other than to
10 exfiltrate or steal, or destroy, use, or modify as part of their ransom attempts, the
11 coveted personal information stored or processed by PMH.

12 18. The personal information exposed by PMH as a result of its inadequate
13 data security is highly valuable on the black market to phishers, hackers, identity
14 thieves, and cybercriminals. Stolen personal information is often trafficked on the
15 "dark web," a heavily encrypted part of the Internet that is not accessible via
16 traditional search engines. Law enforcement has difficulty policing the dark web
17 due to this encryption, which allows users and criminals to conceal identities and
18 online activity.

19 19. When malicious actors infiltrate companies and copy and exfiltrate the
20 personal information that those companies store, or have access to, that stolen
21 information often ends up on the dark web because the malicious actors buy and
22 sell that information for profit.

23 20. The information compromised in this unauthorized cybersecurity
24 attack involves sensitive personal identifying information, which is significantly
25 more valuable than the loss of, for example, credit card information in a retailer
26 data breach because, there, victims can cancel or close credit and debit card
27 accounts. Whereas here, the information compromised is difficult and highly
28 problematic to change—particularly social security numbers.

1 21. Once personal information is sold, it is often used to gain access to
2 various areas of the victim's digital life, including bank accounts, social media,
3 credit card, and tax details. This can lead to additional personal information being
4 harvested from the victim, as well as personal information from family, friends, and
5 colleagues of the original victim.

6 22. Unauthorized data breaches, such as these, facilitate identity theft as
7 hackers obtain consumers' personal information and thereafter use it to siphon
8 money from current accounts, open new accounts in the names of their victims, or
9 sell consumers' personal information to others who do the same.

10 23. Federal and state governments have established security standards and
11 issued recommendations to minimize unauthorized data disclosures and the
12 resulting harm to individuals and financial institutions. Indeed, the Federal Trade
13 Commission ("FTC") has issued numerous guides for businesses that highlight the
14 importance of reasonable data security practices.

15 24. According to the FTC, the need for data security should be factored
16 into all business decision-making.¹ In 2016, the FTC updated its publication,
17 Protecting Personal Information: A Guide for Business, which established
18 guidelines for fundamental data security principles and practices for business.²
19 Among other things, the guidelines note businesses should properly dispose of
20 personal information that is no longer needed, encrypt information stored on
21 computer networks, understand their network's vulnerabilities, and implement
22 policies to correct security problems. The guidelines also recommend that
23 businesses use an intrusion detection system to expose a breach as soon as it occurs,
24 monitor all incoming traffic for activity indicating someone is attempting to hack

25
26 ¹ See Federal Trade Commission, Start with Security (June 2015), available at
<https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last
visited February 3, 2023).

27 ² See Federal Trade Commission, Protecting Personal Information: A Guide for Business (Oct.
28 2016), available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
[0136_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited February 3, 2023).

1 the system, watch for large amounts of data being transmitted from the system, and
2 have a response plan ready in the event of the breach.

3 25. Also, the FTC recommends that companies limit access to sensitive
4 data, require complex passwords to be used on networks, use industry-tested
5 methods for security, monitor for suspicious activity on the network, and verify that
6 third-party service providers have implemented reasonable security measures.³

7 26. Highlighting the importance of protecting against unauthorized data
8 disclosures, the FTC has brought enforcement actions against businesses for failing
9 to adequately and reasonably protect personal information, treating the failure to
10 employ reasonable and appropriate measures to protect against unauthorized access
11 to confidential consumer data as an unfair act or practice prohibited by Section 5 of
12 the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45.

13 27. Orders resulting from these actions further clarify the measures
14 businesses must take to meet their data security obligations.

15 28. The FBI created a technical guidance document for Chief Information
16 Officers and Chief Information Security Officers that compiles already existing
17 federal government and private industry best practices and mitigation strategies to
18 prevent and respond to ransomware attacks. The document is titled *How to Protect*
19 *Your Networks from Ransomware* and states that on average, more than 4,000
20 ransomware attacks have occurred daily since January 1, 2016. Yet, there are very
21 effective prevention and response actions that can significantly mitigate the risks.⁴
22 Preventative measure include:

- 23 • Implement an awareness and training program. Because end users
- 24 are targets, employees and individuals should be aware of the threat
- 25 of ransomware and how it is delivered.
- 26 • Enable strong spam filters to prevent phishing emails from reaching

27 ³ See *id.*

28 ⁴ *How to Protect Your Networks from Ransomware*, FBI, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last viewed February 3, 2023).

the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁵

29. PMH could have prevented the cybersecurity attack by properly

⁵ *Id.*

1 utilizing best practices as advised by the federal government, as described in the
2 preceding paragraphs, but failed to do so.

3 30. PMH's failure to safeguard against a cybersecurity attack is
4 exacerbated by the repeated warnings and alerts from public and private
5 institutions, including the federal government, directed to protecting and securing
6 sensitive data. Experts studying cybersecurity routinely identify companies such as
7 PMH that collect, process, and store massive amounts of data on cloud-based
8 systems as being particularly vulnerable to cyberattacks because of the value of the
9 personal information that they collect and maintain. Accordingly, PMH knew or
10 should have known that it was a prime target for hackers.

11 31. According to the 2021 Thales Global Cloud Security Study, more than
12 40% of organizations experienced a cloud-based data breach in the previous 12
13 months. Yet, despite these incidents, the study found that nearly 83% of cloud-
14 based businesses still fail to encrypt half of the sensitive data they store in the
15 cloud.⁶

16 32. Upon information and belief, PMH did not encrypt Plaintiff's and class
17 members' personal information involved in the data breach.

18 33. Despite knowing the prevalence of data breaches, PMH failed to
19 prioritize cybersecurity by adopting reasonable security measures to prevent and
20 detect unauthorized access to its highly sensitive systems and databases. PMH have
21 the resources to prevent an attack, but neglected to adequately invest in
22 cybersecurity, despite the growing number of well-publicized breaches. PMH failed
23 to fully implement each and all of the above-described data security best practices.
24 PMH further failed to undertake adequate analyses and testing of its own systems,
25 training of its own personnel, and other data security measures to ensure
26 vulnerabilities were avoided or remedied and that Plaintiff's and class members'

27 ⁶ Maria Henriquez, *40% of organizations have suffered a cloud-based data breach*, Security, Oct.
28 29, 2021, <https://www.securitymagazine.com/articles/96412-40-of-organizations-have-suffered-a-cloud-based-datq-breach> (last visited February 3, 2023).

1 data were protected.

2 **Plaintiff's Facts**

3 34. Plaintiff's and class members' personal identifying information,
4 including their name, social security number, date of birth, diagnosis information,
5 lab results, prescription information, treatment information, health insurance
6 information, claims information, and medical record number, among other personal,
7 sensitive and confidential information, were in the possession, custody and/or
8 control of PMH. Plaintiff believed that PMH would protect and keep his personal
9 identifying information protected, secure and safe from unlawful disclosure

10 35. After the data breach, Plaintiff received notice of the data breach from
11 PMH via letter dated September 29, 2023.

12 36. Plaintiff has spent and will continue to spend time and effort
13 monitoring his accounts to protect himself from identity theft. Plaintiff remains
14 concerned for his personal security and the uncertainty of what personal
15 information was exposed to hackers and/or posted to the dark web.

16 37. As a direct and foreseeable result of PMH's negligent failure to
17 implement and maintain reasonable data security procedures and practices and the
18 resultant breach of its systems, Plaintiff and all class members, have suffered harm
19 in that their sensitive personal information has been exposed to cybercriminals and
20 they have an increased stress, risk, and fear of identity theft and fraud. This is not
21 just a generalized anxiety of possible identify theft, privacy, or fraud concerns, but
22 a concrete stress and risk of harm resulting from an actual breach and accompanied
23 by actual instances of reported problems suspected to stem from the breach.

24 38. Upon information and belief, and as detailed in the September 29,
25 2023 notice letter, Plaintiff's name, social security number, date of birth, diagnosis
26 information, lab results, prescription information, treatment information, health
27 insurance information, claims information, and medical record number, among
28 other personal, sensitive and confidential information, and other personal

1 information was exfiltrated by the hackers who obtained unauthorized access to his
2 and class members' personal information for unlawful purposes.

3 39. Social security numbers are among the most sensitive kind of personal
4 information to have stolen because they may be put to a variety of fraudulent uses
5 and are difficult for an individual to change. The Social Security Administration
6 stresses that the loss of an individual's social security number, as is the case here,
7 can lead to identity theft and extensive financial fraud:

8 A dishonest person who has your Social Security number can use it to
9 get other personal information about you. Identity thieves can use
10 your number and your good credit to apply for more credit in your
11 name. Then, they use the credit cards and don't pay the bills, it
12 damages your credit. You may not find out that someone is using your
13 number until you're turned down for credit, or you begin to get calls
14 from unknown creditors demanding payment for items you never
15 bought. Someone illegally using your Social Security number and
16 assuming your identity can cause a lot of problems.⁷

17 40. Furthermore, Plaintiff and class members are well aware that their
18 sensitive personal information, including social security numbers and potentially
19 banking information, risks being available to other cybercriminals on the dark web.
20 Accordingly, all Plaintiff and class members have suffered harm in the form of
21 increased stress, fear, and risk of identity theft and fraud resulting from the data
22 breach. Additionally, Plaintiff and class members have incurred, and/or will incur,
23 out-of-pocket expenses related to credit monitoring and identity theft prevention to
24 address these concerns.

25 **CLASS ACTION ALLEGATIONS**

26 41. Plaintiff brings this action on behalf of himself and all other similarly
27 situated persons pursuant to Federal Rule of Civil Procedure 23, including Rule

28 ⁷ *Identify Theft and Your Social Security Number*, Social Security Administration,
<https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited February 3, 2023).

23(b)(1)-(3) and (c)(4). Plaintiff seeks to represent the following class and subclasses:

Nationwide Class. All persons in the United States whose personal information was compromised in or as a result of PMH's data breach on or around July 31, 2023 through August 3, 2023, which was announced on or around September 29, 2023.

California Subclass. All persons residing in California whose personal information was compromised in or as a result of PMH's data breach on or around July 31, 2023 through August 3, 2023, which was announced on or around September 29, 2023.

Excluded from the class are the following individuals and/or entities: PMH and its parents, subsidiaries, affiliates, officers, directors, or employees, and any entity in which PMH has a controlling interest; all individuals who make a timely request to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

42. Plaintiff reserves the right to amend or modify the class definitions with greater particularity or further division into subclasses or limitation to particular issues.

43. This action has been brought and may be maintained as a class action under Rule 23 because there is a well-defined community of interest in the litigation and the proposed classes are ascertainable, as described further below:

- a. Numerosity: The potential members of the class as defined are so numerous that joinder of all members of the class is impracticable. While the precise number of class members at issue has not been determined, Plaintiff believes the cybersecurity breach affected tens of thousands of individuals nationwide and at least many thousands within California.

1 b. Commonality: There are questions of law and fact common to Plaintiff
2 and the class that predominate over any questions affecting only the
3 individual members of the class. The common questions of law and
4 fact include, but are not limited to, the following:

- 5 i. Whether PMH owed a duty to Plaintiff and class members to
6 exercise due care in collecting, storing, processing, and
7 safeguarding their personal information;
- 8 ii. Whether PMH breached those duties;
- 9 iii. Whether PMH implemented and maintained reasonable security
10 procedures and practices appropriate to the nature of the
11 personal information of class members;
- 12 iv. Whether PMH acted negligently in connection with the
13 monitoring and/or protecting of Plaintiff's and class members'
14 personal information;
- 15 v. Whether PMH knew or should have known that they did not
16 employ reasonable measures to keep Plaintiff's and class
17 members' personal information secure and prevent loss or
18 misuse of that personal information;
- 19 vi. Whether PMH adequately addressed and fixed the
20 vulnerabilities which permitted the data breach to occur;
- 21 vii. Whether PMH caused Plaintiff and class members damages;
- 22 viii. Whether the damages PMH caused to Plaintiff and class
23 members includes the increased risk and fear of identity theft
24 and fraud resulting from the access and exfiltration, theft, or
25 disclosure of their personal information;
- 26 ix. Whether Plaintiff and class members are entitled to credit
27 monitoring and other monetary relief;

- 1 x. Whether PMH's failure to implement and maintain reasonable
2 security procedures and practices constitutes negligence;
3 xi. Whether PMH's failure to implement and maintain reasonable
4 security procedures and practices constitutes negligence per se;
5 xii. Whether PMH's failure to implement and maintain reasonable
6 security procedures and practices constitutes violation of the
7 Federal Trade Commission Act, 15 U.S.C. § 45(a);
8 xiii. Whether PMH's failure to implement and maintain reasonable
9 security procedures and practices constitutes violation of the
10 California Confidentiality of Medical Information Act, Cal. Civ.
11 Code § 56, California's Unfair Competition Law, Cal. Bus. &
12 Prof. Code § 17200; and
13 xiv. Whether the California subclass is entitled to actual pecuniary
14 damages under the private rights of action in the California
15 Customer Records Act, Cal. Civ. Code § 1798.84 and statutory
16 damages under the California Confidentiality of Medical
17 Information Act, Civ. Code § 56, and the proper measure of
18 such damages and/or statutory damages.
- 19 c. Typicality. The claims of the named Plaintiff are typical of the claims
20 of the class members because all had their personal information
21 compromised as a result of PMH's failure to implement and maintain
22 reasonable security measures and the consequent data breach.
- 23 d. Adequacy of Representation. Plaintiff will fairly and adequately
24 represent the interests of the class. Counsel who represent Plaintiff are
25 experienced and competent in consumer and employment class
26 actions, as well as various other types of complex and class litigation.
- 27 e. Superiority and Manageability. A class action is superior to other
28 available means for the fair and efficient adjudication of this

1 controversy. Individual joinder of all Plaintiffs is not practicable, and
2 questions of law and fact common to Plaintiffs predominate over any
3 questions affecting only Plaintiff. Each Plaintiff has been damaged
4 and is entitled to recovery by reason of PMH's unlawful failure to
5 adequately safeguard their data. Class action treatment will allow
6 those similarly situated persons to litigate their claims in the manner
7 that is most efficient and economical for the parties and the judicial
8 system. As any civil penalty awarded to any individual class member
9 may be small, the expense and burden of individual litigation make it
10 impracticable for most class members to seek redress individually. It
11 is also unlikely that any individual consumer would bring an action
12 solely on behalf of himself or herself pursuant to the theories asserted
13 herein. Additionally, the proper measure of civil penalties for each
14 wrongful act will be answered in a consistent and uniform manner.
15 Furthermore, the adjudication of this controversy through a class
16 action will avoid the possibility of inconsistent and potentially
17 conflicting adjudication of the asserted claims. There will be no
18 difficulty in the management of this action as a class action, as PMH's
19 records will readily enable the Court and parties to ascertain affected
20 companies and their employees.

21 f. Notice to Class. Among other means, potential notice to class
22 members of this class action can be accomplished via United States
23 mail to all individuals who received a copy of the September 29, 2023
24 data breach notice letter and/or through electronic mail and/or through
25 publication.

26 44. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and
27 (b)(2) because PMH has acted or refused to act on grounds generally applicable to
28

1 the class, so that final injunctive relief or corresponding declaratory relief is
2 appropriate as to the class as a whole.

3 45. Likewise, particular issues under Rule 23(c)(4) are appropriate for
4 certification because such claims present only particular, common issues, the
5 resolution of which would advance the disposition of the matters and the parties'
6 interests therein. Such particular issues include, but are not limited to:

- 7 a. Whether PMH owed a legal duty to Plaintiff and class members to
8 exercise due care in collecting, storing, processing, using, and
9 safeguarding their personal information;
- 10 b. Whether PMH breached that legal duty to Plaintiff and class members
11 to exercise due care in collecting, storing, processing, using, and
12 safeguarding their personal information;
- 13 c. Whether PMH failed to comply with their own policies and applicable
14 laws, regulations, and industry standards relating to data security;
- 15 d. Whether PMH failed to implement and maintain reasonable security
16 procedures and practices appropriate to the nature of the personal
17 information compromised in the breach; and
- 18 e. Whether class members are entitled to actual damages, credit
19 monitoring, injunctive relief, statutory damages, and/or punitive
20 damages as a result of PMH's wrongful conduct as alleged herein.

21 **FIRST CAUSE OF ACTION**

22 **(Negligence, By Plaintiff and the Nationwide Class Against PMH)**

23 46. Plaintiff realleges and incorporates by reference the preceding
24 paragraphs as if fully set forth herein.

25 47. PMH owed a duty to Plaintiff and class members to exercise
26 reasonable care in obtaining, storing, using, processing, deleting and safeguarding
27 their personal information in its possession from being compromised, stolen,
28 accessed, and/or misused by unauthorized persons. That duty includes a duty to

1 implement and maintain reasonable security procedures and practices appropriate to
2 the nature of the personal information that were compliant with and/or better than
3 industry-standard practices. PMH's duties included a duty to design, maintain, and
4 test its security systems to ensure that Plaintiff's and class members' personal
5 information was adequately secured and protected, to implement processes that
6 would detect a breach of its security system in a timely manner, to timely act upon
7 warnings and alerts, including those generated by its own security systems
8 regarding intrusions to its networks, and to promptly, properly, and fully notify its
9 customers, Plaintiff, and class members of any data breach.

10 48. PMH's duties to use reasonable care arose from several sources,
11 including but not limited to those described below.

12 49. PMH had a common law duty to prevent foreseeable harm to others.
13 This duty existed because Plaintiff and class members were the foreseeable and
14 probable victims of any inadequate security practices. In fact, not only was it
15 foreseeable that Plaintiff and class members would be harmed by the failure to
16 protect their personal information because hackers routinely attempt to steal such
17 information and use it for nefarious purposes, but PMH also knew that it was more
18 likely than not Plaintiff and other class members would be harmed.

19 50. PMH's duty also arose under Section 5 of the Federal Trade
20 Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or
21 affecting commerce," including, as interpreted and enforced by the FTC, the unfair
22 practice of failing to use reasonable measures to protect personal information by
23 companies such as PMH.

24 51. Various FTC publications and data security breach orders further form
25 the basis of PMH's duty. According to the FTC, the need for data security should
26 be factored into all business decision making.⁸ In 2016, the FTC updated its

27
28 ⁸ *Start with Security, A Guide for Business*, FTC (June 2015),
<https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

1 publication, *Protecting Personal Information: A Guide for Business*, which
 2 established guidelines for fundamental data security principles and practices for
 3 business.⁹ Among other things, the guidelines note that businesses should protect
 4 the personal customer information that they keep; properly dispose of personal
 5 information that is no longer needed; encrypt information stored on computer
 6 networks; understand their network's vulnerabilities; and implement policies to
 7 correct security problems. The guidelines also recommend that businesses use an
 8 intrusion detection system to expose a breach as soon as it occurs; monitor all
 9 incoming traffic for activity indicating someone is attempting to hack the system;
 10 watch for large amounts of data being transmitted from the system; and have a
 11 response plan ready in the event of a breach. Additionally, the FTC recommends
 12 that companies limit access to sensitive data, require complex passwords to be used
 13 on networks, use industry-tested methods for security, monitor for suspicious
 14 activity on the network, and verify that third-party service providers have
 15 implemented reasonable security measures. The FBI has also issued guidance on
 16 best practices with respect to data security that also form the basis of PMH's duty
 17 of care, as described above.¹⁰

18 52. By obtaining, collecting, using, and deriving a benefit from Plaintiff's
 19 and class members' personal information, PMH assumed legal and equitable duties
 20 and knew or should have known that it was responsible for protecting Plaintiff's
 21 and class members' personal information from disclosure.

22 53. PMH also had a duty to safeguard the personal information of Plaintiff
 23 and class members and to promptly notify them of a breach because of state laws
 24 and statutes that require PMH to reasonably safeguard personal information, as

25
 26 ⁹ *Protecting Personal Information, A Guide for Business*, FTC (Oct. 2016),
[https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
[information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)

27 ¹⁰ *How to Protect Your Networks from Ransomware*, FBI, [https://www.fbi.gov/file-](https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view)
[repository/ransomware-prevention-and-response-for-cisos.pdf/view](https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view) (last viewed February 3,
 28 2023).

1 detailed herein, including Cal. Civ. Code § 1798.80 *et seq.*

2 54. Timely notification was required, appropriate, and necessary so that,
3 among other things, Plaintiff and class members could take appropriate measures to
4 freeze or lock their credit profiles, cancel or change usernames or passwords on
5 compromised accounts, monitor their account information and credit reports for
6 fraudulent activity, contact their banks or other financial institutions that issue their
7 credit or debit cards, obtain credit monitoring services, develop alternative
8 timekeeping methods or other tacks to avoid untimely or inaccurate wage
9 payments, and take other steps to mitigate or ameliorate the damages caused by
10 PMH's misconduct.

11 55. Plaintiff and class members have taken reasonable steps to maintain
12 the confidentiality of their personal information.

13 56. PMH breached the duties it owed to Plaintiff and class members
14 described above and thus was negligent. PMH breached these duties by, among
15 other things, failing to: (a) exercise reasonable care and implement adequate
16 security systems, protocols and practices sufficient to protect the personal
17 information of Plaintiff and class members; (b) prevent the breach; (c) timely detect
18 the breach; (d) maintain security systems consistent with industry; (e) timely
19 disclose that Plaintiff's and class members' personal information in PMH's
20 possession had been or was reasonably believed to have been stolen or
21 compromised; (f) failing to comply fully even with its own purported security
22 practices.

23 57. PMH knew or should have known of the risks of collecting and storing
24 personal information and the importance of maintaining secure systems, especially
25 in light of the increasing frequency of ransomware attacks. The sheer scope of
26 PMH's operations further shows that PMH knew or should have known of the risks
27 and possible harm that could result from its failure to implement and maintain
28 reasonable security measures. On information and belief, this is but one of the

1 several vulnerabilities that plagued PMH's systems and led to the data breach.

2 58. Through PMH's acts and omissions described in this complaint,
3 including PMH's failure to provide adequate security and its failure to protect the
4 personal information of Plaintiff and class members from being foreseeably
5 captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, PMH
6 unlawfully breached their duty to use reasonable care to adequately protect and
7 secure Plaintiff's and class members' personal information.

8 59. PMH further failed to timely and accurately disclose to customers,
9 Plaintiff, and class members that their personal information had been improperly
10 acquired or accessed and/or was available for sale to criminals on the dark web.
11 PMH has not provided a data breach notice to the Attorney General of California,
12 which would provide statewide notice to impacted individuals. Plaintiff and class
13 members could have taken action to protect their personal information if they were
14 provided timely notice.

15 60. But for PMH's wrongful and negligent breach of its duties owed to
16 Plaintiff and class members, their personal information would not have been
17 compromised.

18 61. Plaintiff and class members relied on PMH to keep their personal
19 information confidential and securely maintained, and to use this information for
20 business purposes only, and to make only authorized disclosures of this
21 information.

22 62. As a direct and proximate result of PMH's negligence, Plaintiff and
23 class members have been injured as described herein, and are entitled to damages,
24 including compensatory, punitive, and nominal damages, in an amount to be proven
25 at trial. As a result of PMH's failure to protect Plaintiff's and class members'
26 personal information, Plaintiff's and class members' personal information has been
27 accessed by malicious cybercriminals. Plaintiff's and the class members' injuries
28 include:

- a. theft of their personal information;
- b. costs associated with requested credit freezes;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. costs associated with purchasing credit monitoring and identity theft protection services;
- e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- f. lowered credit scores resulting from credit inquiries following fraudulent activities;
- g. costs associated with time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;
- h. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information being placed in the hands of criminals;
- i. damages to and diminution of value of their personal information entrusted, directly or indirectly, to PMH with the mutual understanding that PMH would safeguard Plaintiff's and the class members' data against theft and not allow access and misuse of their data by others;

- j. continued risk of exposure to hackers and thieves of their personal information, which remains in PMH's possession and is subject to further breaches so long as PMH fails to undertake appropriate and adequate measures to protect Plaintiff and class members, along with damages stemming from the stress, fear, and anxiety of an increased risk of identity theft and fraud stemming from the breach;
- k. loss of the inherent value of their personal information;
- l. the loss of the opportunity to determine for themselves how their personal information is used; and
- m. other significant additional risk of identity theft, financial fraud, and other identity-related fraud in the indefinite future.

63. In connection with the conduct described above, PMH acted wantonly, recklessly, and with complete disregard for the consequences Plaintiff and class members would suffer if their highly sensitive and confidential personal information, including but not limited to name, company name, address, social security numbers, and banking and credit card information, was access by unauthorized third parties.

SECOND CAUSE OF ACTION

(Negligence Per Se, By Plaintiff and the Nationwide Class Against PMH)

64. Plaintiff realleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

65. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as PMH. Various FTC publications and data security breach orders further form the basis of PMH's duty. In addition, individual states have enacted statutes based on the FTC Act that also created a duty.

1 regarding its present and prospective common law and other duties to reasonably
2 safeguard consumers personal identifying information in its possession, custody
3 and/or control and regarding whether PMH is currently maintaining data security
4 measures adequate to protect Plaintiff and class members from further data
5 breaches that compromise their personal information. Plaintiff alleges that PMH's
6 data security measures remain inadequate. PMH denies these allegations. Plaintiff
7 continues to suffer injury as a result of the compromise of his personal information
8 and remains at imminent risk that further compromises of her personal information
9 will occur in the future.

10 74. Pursuant to its authority under the Declaratory Judgment Act, this
11 Court should enter a judgment declaring, among other things, the following:

- 12 a. PMH continues to owe a legal duty to secure consumers' personal
13 information, including Plaintiff's and class members' personal
14 information, to timely notify them of a data breach under the common
15 law, Section 5 of the FTC Act; and
16 b. PMH continues to breach this legal duty by failing to employ
17 reasonable measures to secure Plaintiff's and class members' personal
18 information.

19 75. The Court should issue corresponding prospective injunctive relief
20 requiring PMH to employ adequate security protocols consistent with law and
21 industry standards to protect Plaintiff's and class members' personal information.

22 76. If an injunction is not issued, Plaintiff will suffer irreparable injury,
23 and lack an adequate legal remedy, in the event of another data breach at PMH.
24 The risk of another such breach is real, immediate, and substantial. If another
25 breach at PMH occurs, Plaintiff will not have an adequate remedy at law because
26 many of the resulting injuries are not readily quantified and they will be forced to
27 bring multiple lawsuits to rectify the same conduct.

28 77. The hardship to Plaintiff if an injunction does not issue exceeds the

1 hardship to PMH if an injunction is issued. Among other things, if another massive
 2 data breach occurs, Plaintiff and class members will likely be subjected to
 3 substantial identity theft and other damage. On the other hand, the cost to PMH of
 4 complying with an injunction by employing reasonable prospective data security
 5 measures is relatively minimal, and PMH has a pre-existing legal obligation to
 6 employ such measures.

7 78. Issuance of the requested injunction will not disserve the public
 8 interest. To the contrary, such an injunction would benefit the public by preventing
 9 another data breach, thus eliminating the additional injuries that would result to
 10 Plaintiff and the thousands of class members whose confidential information would
 11 be further compromised.

12
 13 **FOURTH CAUSE OF ACTION**
 14 **(Violation of the California Confidentiality of Medical Information Act**
 15 **("CMIA"), Cal. Civ. Code § 56, *et seq.***
 16 **By Plaintiff and the California Class Against All Defendants)**

17 79. Plaintiff realleges and incorporates by reference the preceding
 18 paragraphs as though fully set forth herein.

19 80. Section 56.10(a) of the California Civil Code provides that "[a]
 20 provider of health care, health care service plan, or contractor shall not disclose
 21 medical information regarding a patient of the provider of health care or an enrollee
 22 or subscriber of a health care service plan without first obtaining an
 23 authorization[.]"

24 81. PMH is a "contractor" within the meaning of Civil Code § 56.05(d)
 25 within the meaning of Civil Code § 56.06 and/or a "business organized for the
 26 purpose of maintaining medical information" and/or a "business that offers software
 27 or hardware to consumers . . . that is designed to maintain medical information"
 28 within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues
 to maintain "medical information," within the meaning of Civil Code § 56.05(j), for

1 "patients" of PMH, within the meaning of Civil Code § 56.05(k).

2 82. Plaintiff and class members are "patients" within the meaning of Civil
3 Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code §
4 56.05(e) because Plaintiff and Class members fear that disclosure of their medical
5 information could subject them to harassment or abuse.

6 83. Plaintiff and class members, as patients, had their individually
7 identifiable "medical information," within the meaning of Civil Code § 56.05(j),
8 created, maintained, preserved, and stored on PMH's computer network at the time
9 of the unauthorized disclosure.

10 84. PMH, through inadequate security, allowed unauthorized third-party
11 access to Plaintiff's and class members' medical information, without the prior
12 written authorization of Plaintiff and class members, as required by Civil Code §
13 56.10 of the CMIA.

14 85. In violation of Civil Code § 56.10(a), PMH disclosed Plaintiff's and
15 class members' medical information without first obtaining an authorization.
16 Plaintiff's and class members' medical information was viewed by unauthorized
17 individuals as a direct and proximate result of PMH's violation of Civil Code §
18 56.10(a).

19 86. In violation of Civil Code § 56.10(e), PMH further disclosed Plaintiff's
20 and class members' medical information to persons or entities not engaged in
21 providing direct health care services to Plaintiff or class members, or to their
22 providers of health care or health care service plans or their insurers or self-insured
23 employers.

24 87. PMH violated Civil Code § 56.101 of the CMIA through its willful
25 and knowing failure to maintain and preserve the confidentiality of the medical
26 information of Plaintiff and the class members. PMH's conduct with respect to the
27 disclosure of confidential PII/PHI was willful and knowing because PMH designed
28 and implemented the computer network and security practices that gave rise to the

1 unlawful disclosure.

2 88. In violation of Civil Code § 56.101(a), PMH created, maintained,
3 preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and class
4 members' medical information in a manner that failed to preserve and breached the
5 confidentiality of the information contained therein. Plaintiff's and class members'
6 medical information was viewed by unauthorized individuals as a direct and
7 proximate result of PMH's violation of Civil Code § 56.101(a). 380. In violation of
8 Civil Code § 56.101(a), PMH negligently created, maintained, preserved, stored,
9 abandoned, destroyed, or disposed of Plaintiff's and class members' medical
10 information. Plaintiff's and class members' medical information was viewed by
11 unauthorized individuals as a direct and proximate result of PMH's violation of
12 Civil Code § 56.101(a).

13 89. Plaintiff's and class members' medical information that was the subject
14 of the unauthorized disclosure included "electronic medical records" or "electronic
15 health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. §
16 17921(5).

17 90. In violation of Civil Code § 56.101(b)(1)(A), PMH's electronic health
18 record system or electronic medical record system failed to protect and preserve the
19 integrity of electronic medical information. Plaintiff's and class members' medical
20 information was viewed by unauthorized individuals as a direct and proximate
21 result of PMH's violation of Civil Code § 56.101(b)(1)(A).

22 91. PMH violated Civil Code § 56.36 of the CMIA through its failure to
23 maintain and preserve the confidentiality of the medical information of Plaintiff and
24 the class members.

25 92. As a result of PMH's above-described conduct, Plaintiff and class
26 members have suffered damages from the unauthorized disclosure and release of
27 their individual identifiable "medical information" made unlawful by Civil Code §§
28 56.10, 56.101, 56.36. 385. As a direct and proximate result of PMH's above-

described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the unauthorized disclosure, and violation of the CMIA, Plaintiff and class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud-risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

93. Plaintiff, individually and for each member of the class, seeks nominal damages of one thousand dollars (\$1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to \$3,000 per Plaintiff and each class member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

FIFTH CAUSE OF ACTION
(Violation of the California Customer Records Act, Cal. Civ. Code §§ 1798.80
et seq.,
By Plaintiff and the California Subclass Against PMH)

94. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

95. Cal. Civ. Code § 1798.81.5 provides that “[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide

1 reasonable security for that information.”

2 96. Section 1798.81.5(b) further states that: “[a] business that owns,
3 licenses, or maintains personal information about a California resident shall
4 implement and maintain reasonable security procedures and practices appropriate to
5 the nature of the information, to protect the personal information from unauthorized
6 access, destruction, use, modification, or disclosure.”

7 97. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a
8 violation of this title may institute a civil action to recover damages.” Section
9 1798.84(e) further provides that “[a]ny business that violates, proposes to violate,
10 or has violated this title may be enjoined.”

11 98. Plaintiff and members of the California subclass are “customers”
12 within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are
13 individuals who provided personal information to PMH, directly and/or indirectly,
14 for the purpose of obtaining a service from PMH.

15 99. The personal information of Plaintiff and the California subclass at
16 issue in this lawsuit constitutes “personal information” under § 1798.81.5(d)(1) in
17 that the personal information PMH collects and which was impacted by the
18 cybersecurity attack includes an individual’s first name or first initial and the
19 individual’s last name in combination with one or more of the following data
20 elements, with either the name or the data elements not encrypted or redacted: (i)
21 Social security number; (ii) Driver’s license number, California identification card
22 number, tax identification number, passport number, military identification number,
23 or other unique identification number issued on a government document commonly
24 used to verify the identity of a specific individual; (iii) account number or credit or
25 debit card number, in combination with any required security code, access code, or
26 password that would permit access to an individual’s financial account; (iv) medical
27 information; (v) health insurance information; (vi) unique biometric data generated
28 from measurements or technical analysis of human body characteristics, such as a

1 fingerprint, retina, or iris image, used to authenticate a specific individual.

2 100. PMH knew or should have known that its computer systems and data
3 security practices were inadequate to safeguard the California subclass's personal
4 information and that the risk of a data breach or theft was highly likely. PMH
5 failed to implement and maintain reasonable security procedures and practices
6 appropriate to the nature of the information to protect the personal information of
7 Plaintiff and the California subclass. Specifically, PMH failed to implement and
8 maintain reasonable security procedures and practices appropriate to the nature of
9 the information, to protect the personal information of Plaintiff and the California
10 subclass from unauthorized access, destruction, use, modification, or disclosure.
11 PMH further subjected Plaintiff's and the California subclass's nonencrypted and
12 nonredacted personal information to an unauthorized access and exfiltration, theft,
13 or disclosure as a result of the PMH's violation of the duty to implement and
14 maintain reasonable security procedures and practices appropriate to the nature of
15 the information, as described herein.

16 101. As a direct and proximate result of PMH's violation of its duty, the
17 unauthorized access, destruction, use, modification, or disclosure of the personal
18 information of Plaintiff and the California subclass included hackers' access to,
19 removal, deletion, destruction, use, modification, disabling, disclosure and/or
20 conversion of the personal information of Plaintiff and the California subclass by
21 the ransomware attackers and/or additional unauthorized third parties to whom
22 those cybercriminals sold and/or otherwise transmitted the information.

23 102. As a direct and proximate result of PMH's acts or omissions, Plaintiff
24 and the California subclass were injured and lost money or property including, but
25 not limited to, the loss of Plaintiff's and the subclass's legally protected interest in
26 the confidentiality and privacy of their personal information, nominal damages, and
27 additional losses described above. Plaintiff seeks compensatory damages as well as
28 injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

1 103. Moreover, the California Customer Records Act further provides: “A
2 person or business that maintains computerized data that includes personal
3 information that the person or business does not own shall notify the owner or
4 licensee of the information of the breach of the security of the data immediately
5 following discovery, if the personal information was, or is reasonably believed to
6 have been, acquired by an unauthorized person.” Cal. Civ. Code § 1798.82.

7 104. Any person or business that is required to issue a security breach
8 notification under the CRA must meet the following requirements under
9 §1798.82(d):

- 10 a. The name and contact information of the reporting person or business
11 subject to this section;
- 12 b. A list of the types of personal information that were or are reasonably
13 believed to have been the subject of a breach;
- 14 c. If the information is possible to determine at the time the notice is
15 provided, then any of the following:
 - 16 i. the date of the breach,
 - 17 ii. the estimated date of the breach, or
 - 18 iii. the date range within which the breach occurred. The
19 notification shall also include the date of the notice;
- 20 d. Whether notification was delayed as a result of a law enforcement
21 investigation, if that information is possible to determine at the time
22 the notice is provided;
- 23 e. A general description of the breach incident, if that information is
24 possible to determine at the time the notice is provided;
- 25 f. The toll-free telephone numbers and addresses of the major credit
26 reporting agencies if the breach exposed a social security number or a
27 driver’s license or California identification card number;
- 28 g. If the person or business providing the notification was the source of

1 the breach, an offer to provide appropriate identity theft prevention and
2 mitigation services, if any, shall be provided at no cost to the affected
3 person for not less than 12 months along with all information
4 necessary to take advantage of the offer to any person whose
5 information was or may have been breached if the breach exposed or
6 may have exposed personal information.

7 105. PMH failed to provide the legally compliant notice under § 1798.82(d)
8 to Plaintiff and members of the California subclass. On information and belief, to
9 date, PMH has not sent written notice of the data breach to all impacted individuals.
10 As a result, PMH has violated § 1798.82 by not providing legally compliant and
11 timely notice to all class members. Because not all members of the class have been
12 notified of the breach, members could have taken action to protect their personal
13 information, but were unable to do so because they were not timely notified of the
14 breach.

15 106. On information and belief, many class members affected by the
16 breach, have not received any notice at all from PMH in violation of Section
17 1798.82(d).

18 107. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and
19 class members suffered incrementally increased damages separate and distinct from
20 those simply caused by the breaches themselves.

21 108. As a direct consequence of the actions as identified above, Plaintiff
22 and class members incurred additional losses and suffered further harm to their
23 privacy, including but not limited to economic loss, the loss of control over the use
24 of their identity, increased stress, fear, and anxiety, harm to their constitutional right
25 to privacy, lost time dedicated to the investigation of the breach and effort to cure
26 any resulting harm, the need for future expenses and time dedicated to the recovery
27 and protection of further loss, and privacy injuries associated with having their
28 sensitive personal, financial, and payroll information disclosed, that they would not

1 have otherwise incurred, and are entitled to recover compensatory damages
2 according to proof pursuant to § 1798.84(b).

3
4 **SIXTH CAUSE OF ACTION**
5 **(Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code**
6 **§17200 *et seq.***
7 **By Plaintiff and the California Subclass Against PMH)**

8 109. Plaintiff realleges and incorporates by reference the preceding
9 paragraphs as though fully set forth herein.

10 110. PMH is a “person” defined by Cal. Bus. & Prof. Code § 17201.

11 111. PMH violated Cal. Bus. & Prof. Code § 17200 *et seq.* (“UCL”) by
12 engaging in unlawful, unfair, and deceptive business acts and practices.

13 112. PMH’ “unfair” acts and practices include:

- 14 a. PMH failed to implement and maintain reasonable security measures
15 to protect Plaintiff’s and California subclass members’ personal
16 information from unauthorized disclosure, release, data breaches, and
17 theft, which was a direct and proximate cause of the PMH data breach.
18 PMH failed to identify foreseeable security risks, remediate identified
19 security risks, and adequately improve security following previous
20 cybersecurity incidents and known coding vulnerabilities in the
21 industry;
- 22 b. PMH’s failure to implement and maintain reasonable security
23 measures also was contrary to legislatively-declared public policy that
24 seeks to protect consumers’ data and ensure that entities that are
25 trusted with it use appropriate security measures. These policies are
26 reflected in laws, including the FTC Act (15 U.S.C. § 45), California’s
27 Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and
28 California’s Confidentiality of Medical Information Act (Cal. Civ.
Code § 56);

1 c. PMH's failure to implement and maintain reasonable security
2 measures also led to substantial consumer injuries, as described above,
3 that are not outweighed by any countervailing benefits to consumers or
4 competition. Moreover, because consumers could not know of PMH's
5 inadequate security, consumers could not have reasonably avoided the
6 harms that PMH caused; and

7 d. Engaging in unlawful business practices by violating Cal. Civ. Code §
8 1798.82.

9 113. PMH has engaged in "unlawful" business practices by violating
10 multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§
11 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring
12 timely breach notification), California's Confidentiality of Medical Information Act
13 (Cal. Civ. Code § 56), California's Consumers Legal Remedies Act, Cal. Civ. Code
14 §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law.

15 114. PMH's unlawful, unfair, and deceptive acts and practices include:

16 a. Failing to implement and maintain reasonable security and privacy
17 measures to protect Plaintiff's and California subclass members'
18 personal information, which was a direct and proximate cause of the
19 PMH data breach;

20 b. Failing to identify foreseeable security and privacy risks, remediate
21 identified security and privacy risks, and adequately improve security
22 and privacy measures following previous cybersecurity incidents,
23 which was a direct and proximate cause of the PMH data breach;

24 c. Failing to comply with common law and statutory duties pertaining to
25 the security and privacy of Plaintiff's and California subclass
26 members' personal information, including duties imposed by the FTC
27 Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ.
28 Code §§ 1798.80 *et seq.*, and California's Confidentiality of Medical

1 Information Act (Cal. Civ. Code § 56), which was a direct and
2 proximate cause of the PMH data breach;

- 3 d. Misrepresenting that it would protect the privacy and confidentiality of
4 Plaintiff's and California subclass members' personal information,
5 including by implementing and maintaining reasonable security
6 measures;
- 7 e. Misrepresenting that it would comply with common law and statutory
8 duties pertaining to the security and privacy of Plaintiff's and
9 California subclass members' personal information, including duties
10 imposed by the FTC Act, 15 U.S.C. § 45, California's Customer
11 Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, and California's
12 Confidentiality of Medical Information Act (Cal. Civ. Code § 56);
- 13 f. Omitting, suppressing, and concealing the material fact that it did not
14 reasonably or adequately secure Plaintiff's and California subclass
15 members' personal information; and
- 16 g. Omitting, suppressing, and concealing the material fact that it did not
17 comply with common law and statutory duties pertaining to the
18 security and privacy of Plaintiff's and California subclass members'
19 personal information, including duties imposed by the FTC Act, 15
20 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§
21 1798.80, *et seq.*, and California's Confidentiality of Medical
22 Information Act (Cal. Civ. Code § 56).

23 115. PMH's representations and omissions were material because they
24 were likely to deceive reasonable consumers about the adequacy of PMH's data
25 security and ability to protect the confidentiality of consumers' personal
26 information.

27 116. As a direct and proximate result of PMH's unfair, unlawful, and
28 fraudulent acts and practices, Plaintiff and California subclass members were

1 injured and lost money or property, which would not have occurred but for the
 2 unfair and deceptive acts, practices, and omissions alleged herein, monetary
 3 damages from fraud and identity theft, time and expenses related to monitoring
 4 their financial accounts for fraudulent activity, an increased, imminent risk of fraud
 5 and identity theft, and loss of value of their personal information.

6 117. PMH's violations were, and are, willful, deceptive, unfair, and
 7 unconscionable.

8 118. Plaintiff and class members have lost money and property as a result
 9 of PMH's conduct in violation of the UCL, as stated herein and above.

10 119. By deceptively storing, collecting, and disclosing their personal
 11 information, PMH has taken money or property from Plaintiff and class members.

12 120. PMH acted intentionally, knowingly, and maliciously to violate
 13 California's Unfair Competition Law, and recklessly disregarded Plaintiff's and
 14 California subclass members' rights. Past data breaches put it on notice that its
 15 security and privacy protections were inadequate.

16 121. Plaintiff and California subclass members seek all monetary and
 17 nonmonetary relief allowed by law, including restitution of all profits stemming
 18 from PMH's unfair, unlawful, and fraudulent business practices or use of their
 19 personal information; declaratory relief; reasonable attorneys' fees and costs under
 20 California Code of Civil Procedure § 1021.5; injunctive relief; and other
 21 appropriate equitable relief, including public injunctive relief.

22 **SEVENTH CAUSE OF ACTION**
 23 **(Invasion of Privacy)**

24 **(Count 1 – Common Law Invasion of Privacy – Intrusion Upon Seclusion**
 25 **By Plaintiff and the Nationwide Class Against PMH)**

26 122. Plaintiff realleges and incorporates by reference the preceding
 27 paragraphs as though fully set forth herein.

28 123. To assert claims for intrusion upon seclusion, one must plead (1) that

1 the defendant intentionally intruded into a matter as to which plaintiff had a
2 reasonable expectation of privacy; and (2) that the intrusion was highly offensive to
3 a reasonable person.

4 124. PMH intentionally intruded upon the solitude, seclusion and private
5 affairs of Plaintiff and class members by intentionally configuring their systems in
6 such a way that left them vulnerable to malware/ransomware attack, thus permitting
7 unauthorized access to their systems, which compromised Plaintiff's and class
8 members' personal information. Only PMH had control over its systems.

9 125. PMH's conduct is especially egregious and offensive as they failed to
10 have adequate security measures in place to prevent, track, or detect in a timely
11 fashion unauthorized access to Plaintiff's and class members' personal information.

12 126. At all times, PMH was aware that Plaintiff's and class members'
13 personal information in their possession contained highly sensitive and confidential
14 personal information.

15 127. Plaintiff and class members have a reasonable expectation of privacy
16 in their personal information, which also contains highly sensitive medical
17 information.

18 128. PMH intentionally configured their systems in such a way that stored
19 Plaintiff's and class members' personal information to be left vulnerable to
20 malware/ransomware attack without regard for Plaintiff's and class members'
21 privacy interests.

22 129. The disclosure of the sensitive and confidential personal information
23 of thousands of consumers, was highly offensive to Plaintiff and class members
24 because it violated expectations of privacy that have been established by general
25 social norms, including by granting access to information and data that is private
26 and would not otherwise be disclosed.

27 130. PMH's conduct would be highly offensive to a reasonable person in
28 that it violated statutory and regulatory protections designed to protect highly

1 sensitive information, in addition to social norms. PMH's conduct would be
2 especially egregious to a reasonable person as PMH publicly disclosed Plaintiff's
3 and class members' sensitive and confidential personal information without their
4 consent, to an "unauthorized person," i.e., hackers.

5 131. As a result of PMH's actions, Plaintiff and class members have
6 suffered harm and injury, including but not limited to an invasion of their privacy
7 rights.

8 132. Plaintiff and class members have been damaged as a direct and
9 proximate result of PMH's intrusion upon seclusion and are entitled to just
10 compensation.

11 133. Plaintiff and class members are entitled to appropriate relief, including
12 compensatory damages for the harm to their privacy, loss of valuable rights and
13 protections, and heightened stress, fear, anxiety and risk of future invasions of
14 privacy.

15 **(Count 2 –Invasion of Privacy – Cal. Const. Art. 1, § 1**
16 **By Plaintiff and the California Subclass Against PMH)**

17 134. Plaintiff realleges and incorporates by reference the preceding
18 paragraphs as though fully set forth herein.

19 135. Art. I, § 1 of the California Constitution provides: "All people are by
20 nature free and independent and have inalienable rights. Among these are enjoying
21 and defending life and liberty, acquiring, possessing, and protecting property, and
22 pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

23 136. The right to privacy in California's constitution creates a private right
24 of action against private and government entities.

25 137. To state a claim for invasion of privacy under the California
26 Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a
27 reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope,
28 and actual or potential impact as to constitute an egregious breach of the social

1 norms.

2 138. PMH violated Plaintiff's and class members' constitutional right to
3 privacy by collecting, storing, and disclosing their personal information in which
4 they had a legally protected privacy interest, and in which they had a reasonable
5 expectation of privacy in, in a manner that was highly offensive to Plaintiff and
6 class members, would be highly offensive to a reasonable person, and was an
7 egregious violation of social norms.

8 139. PMH has intruded upon Plaintiff's and class members' legally
9 protected privacy interests, including interests in precluding the dissemination or
10 misuse of their confidential personal information.

11 140. PMH's actions constituted a serious invasion of privacy that would be
12 highly offensive to a reasonable person in that: (i) the invasion occurred within a
13 zone of privacy protected by the California Constitution, namely the misuse of
14 information gathered for an improper purpose; and (ii) the invasion deprived
15 Plaintiff and class members of the ability to control the circulation of their personal
16 information, which is considered fundamental to the right to privacy.

17 141. Plaintiff and class members had a reasonable expectation of privacy in
18 that: (i) PMH's invasion of privacy occurred as a result of PMH's security practices
19 including the collecting, storage, and unauthorized disclosure of consumers'
20 personal information; (ii) Plaintiff and class members did not consent or otherwise
21 authorize PMH to disclose their personal information; and (iii) Plaintiff and class
22 members could not reasonably expect PMH would commit acts in violation of laws
23 protecting privacy.

24 142. As a result of PMH's actions, Plaintiff and class members have been
25 damaged as a direct and proximate result of PMH's invasion of their privacy and
26 are entitled to just compensation.

27 143. Plaintiff and class members suffered actual and concrete injury as a
28 result of PMH's violations of their privacy interests. Plaintiff and class members

are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

144. Plaintiff and class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and class members for the harm to their privacy interests as well as disgorgement of profits made by PMH as a result of its intrusions upon Plaintiff's and class members' privacy.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself, the nationwide class, and the California subclass, prays for the following relief:

1. An order certifying the nationwide class and California subclass as defined above pursuant to Fed. R. Civ. P. 23 and declaring that Plaintiff is proper class representative and appointing Plaintiff's counsel as class counsel;
2. Permanent injunctive relief to prohibit PMH from continuing to engage in the unlawful acts, omissions, and practices described herein;
3. Compensatory, consequential, general, and nominal damages in an amount to be proven at trial, in excess of \$5,000,000;
4. Disgorgement and restitution of all earnings, profits, compensation, and benefits received as a result of the unlawful acts, omissions, and practices described herein;
5. Punitive, exemplary, and/or trebled damages to the extent permitted by law;
6. Statutory damages pursuant to Cal. Civ. Code § 56.36(b);
7. A declaration of right and liabilities of the parties;

1 8. Costs of suit;

2 9. Reasonable attorneys' fees, including pursuant to Cal. Civ. Pro. Code §
3 1021.5;

4 10. Pre- and post-judgment interest at the maximum legal rate;

5 11. Distribution of any monies recovered on behalf of members of the class or
6 the general public via fluid recovery or *cy pres* recovery where necessary
7 and as applicable to prevent Defendant from retaining the benefits of their
8 wrongful conduct; and

9 12. Such other relief as the Court deems just and proper.

10 Dated: October 3, 2023

WUCETICH & KOROVILAS LLP

11 By: /s/ Jason M. Wucetich

12 JASON M. WUCETICH
13 Attorneys for Plaintiff
14 JOSHUA STRADINGER,
15 individually and on behalf of
16 all others similarly situated
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the putative class and subclass, hereby demands a trial by jury on all issues of fact or law so triable.

Dated: October 3, 2023

WUCETICH & KOROVILAS LLP

By: /s/ Jason M. Wucetich

JASON M. WUCETICH
Attorneys for Plaintiff
JOSHUA STRADINGER,
individually and on behalf of
all others similarly situated